

ECHELON:

PART TWO:

THE NSA'S GLOBAL SPYING NETWORK

By Patrick S. Poole

Excerpts from Nexus Magazine Oct/Nov 1999

The US National Security Agency uses the ECHELON system not only for surveillance of civilians and politicians, but also for spying on behalf of US corporations.

A fundamental foundation of free societies is that when controversies arise over the assumption of power by the state, power never defaults to the government, nor are powers granted without an extraordinary, explicit and compelling public interest. As the late United States Supreme Court Justice William Brennan pointed out:



The concept of military necessity is seductively broad and has a dangerous plasticity. Because they invariably have the visage of overriding importance, there is always a temptation to invoke security "necessities" to justify an encroachment upon civil liberties. For that reason, the military-security argument must be approached with a healthy scepticism: its very gravity counsels that courts be cautious when military necessity is invoked by the Government to justify a trespass on [Constitutional] rights.

Despite the necessity of confronting terrorism and the many benefits that are provided by the massive surveillance efforts embodied by **ECHELON**, there is a dark and dangerous side of these activities that is concealed by the cloak of secrecy surrounding the intelligence operations of the United States.

The discovery of domestic surveillance targeting American civilians for reasons of "unpopular" political affiliation or for no probable cause at all - in violation of the First, Fourth and Fifth Amendments of the Constitution - is regularly impeded by very elaborate and complex legal arguments and privilege claims by the intelligence agencies and the US Government. The guardians and caretakers of our liberties - our duly elected political representatives - give scarce attention to the activities, let alone the

abuses, that occur under their watch. As pointed out below, our elected officials frequently become targets of **ECHELON** themselves, chilling any effort to check this unbridled power.

In addition, the shift in priorities resulting from the demise of the Soviet Empire, and the necessity to justify intelligence capabilities, resulted in a redefinition of "national security interests" to include espionage committed on behalf of powerful American companies. This quiet collusion between political and private interests typically involves the very same companies that are involved in developing the technology that empowers **ECHELON** and the intelligence agencies.

DOMESTIC AND POLITICAL SYPING

When considering the use of **ECHELON** on American soil, the pathetic historical record of NSA and CIA domestic activities in regard to the Constitutional liberties and privacy rights of American citizens provides an excellent guidepost for what may occur now with the **ECHELON** system. Since the creation of the NSA by President Truman, its spying capability has frequently been used to monitor the activities of an unsuspecting public.

PROJECT SHAMROCK

In 1945, Project SHAMROCK was initiated to obtain copies of all telegraphic information exiting or entering the United States. With the full cooperation of RCA, ITT and Western Union (representing almost all of the telegraphic traffic in the US at the time), the NSA's predecessor and later the NSA itself were provided with daily microfilm copies of all incoming, outgoing and transiting telegraphs. This system changed dramatically when the cable companies began providing magnetic computer tapes to the agency, which enabled the agency to run all the messages through its HARVEST computer to look for particular keywords, locations, senders or addresses.

Project SHAMROCK became so successful that in 1966 the NSA and CIA set up a front company in lower Manhattan (where the offices of the telegraph companies were located) under the code-name LPMEDLEY. At the height of Project SHAMROCK, 150,000 messages a month were printed and analysed by NSA agents.

NSA Director Lew Allen brought Project SHAMROCK to a crashing halt in May 1975 as congressional critics began to rip open the program's shroud of secrecy. The testimony of both the representatives from the cable companies and Director Allen at the hearings prompted Senate Intelligence Committee chairman Senator Frank Church to conclude that Project SHAMROCK was "probably the largest government interception program affecting Americans ever undertaken".

PROJECT MINARET

A sister project to Project SHAMROCK, Project MINARET involved the creation of "watch lists", by each of the intelligence agencies and the FBI, of those accused of "subversive" domestic activities. The watch lists included such notables as Martin Luther King, Malcolm X, Jane Fonda, Joan Baez and Dr. Benjamin Spock.

After the Supreme Court handed down its 1972 Keith decision - which held that, while the President could act to protect the country from unlawful and subversive activity designed to overthrow the government, that same power did not extend to include warrantless electronic surveillance of domestic organisations - pressure came to bear on Project MINARET. Attorney General Elliot Petersen shut down Project MINARET as soon as its activities were revealed to the Justice Department, despite the fact that the FBI (an agency under the Justice Department's authority) was actively involved with the NSA and other intelligence agencies in creating the watch lists.

Operating between 1967 and 1973, over 5,925 foreigners and 1,690 organisations and US citizens were included on the Project MINARET watch lists. Despite extensive efforts to conceal the NSA's involvement in Project MINARET, NSA Director Lew Allen testified before the Senate Intelligence Committee in 1975 that the NSA had issued over 3,900 reports on the watch-listed Americans. Additionally, the NSA Office of Security Services maintained reports on at least 75,000 Americans between 1952 and 1974. This list included the names of anyone who was mentioned in an NSA message intercept.

OPERATION CHAOS

While the NSA was busy snooping on US citizens through Projects SHAMROCK and MINARET, the CIA got into the domestic spying act by initiating Operation CHAOS. President Lyndon Johnson authorised the creation of the CIA's Domestic Operations Division (DOD), whose purpose was to "exercise centralised responsibility for direction, support and coordination of clandestine cooperations activities within the United States".

When Johnson ordered CIA Director John McCone to use the DOD to analyse the growing college student protests against the Administration's policy towards Vietnam, two new units were set up to target anti-war protesters and organisations: Project RESISTANCE, which worked with college administrators, campus security and local police to identify anti-war activists and political dissidents; and Project MERRIMAC, which monitored any demonstrations being conducted in the Washington, DC, area. The CIA then began monitoring student activists and infiltrating anti-war organisations by working with local police departments to pull-off burglaries, illegal entries (black bag jobs), interrogations and electronic surveillance. After President Nixon came to office in 1969, all of these domestic surveillance activities were consolidated into Operation CHAOS.

After the revelation of two former CIA agents' involvement in the Watergate break-in, the publication of an article about CHAOS in the New York Times and the growing concern about distancing itself from illegal domestic spying activities, the CIA shut down Operation CHAOS. But during the life of the project, the Church Committee and the Commission on CIA Activities within the United States (the Rockefeller Commission) revealed that the CIA had compiled files on over 13,000 individuals, including 7,000 US citizens and 1,000 domestic organisations.

The Foreign Intelligence Surveillance Court (FISC)

In response to the discovery of such a comprehensive effort by previous administrations and the intelligence agencies, Congress passed legislation (the Foreign Intelligence Surveillance Act of 1978) that created a top-secret court, the Foreign Intelligence Surveillance Court (FISC), to hear applications for electronic surveillance from the FBI and NSA to provide some check on the domestic activities of the agencies. In 1995, Congress granted the court additional power to authorise surreptitious entries. In all of these actions, congressional intent was to provide a check on the domestic surveillance abuses mentioned above.

The seven-member court, comprised of Federal District Court judges appointed by the Supreme Court Chief Justice, sits in secret in a sealed room on the top floor of the Department of Justice building. Public information about the FISC's hearings is scarce, but each year the Attorney-General is required by law to transmit to Congress a report detailing the number of applications each year and the number granted.

With over 10,000 applications submitted to the FISC during the past 20 years, the court has only rejected one application (and that rejection was at the request of the Reagan Administration, which had submitted the application).

While the FISC was established to be the watchdog for the Constitutional rights of the American people against domestic surveillance, it quickly became the lap dog of the intelligence agencies. Surveillance requests that would never receive a hearing in a state or federal court are routinely approved by the FISC. This has allowed the FBI to use the process to conduct surveillance to obtain evidence in circumvention of the US Constitution, the evidence then being used in subsequent criminal trials. But the process established by Congress and the courts ensures that information regarding the cause or extent of the surveillance order is withheld from defence attorneys because of the classified nature of the court. Despite Congress's initial intent for the FISC, it is doubtful that domestic surveillance by means of **ECHELON** comes under any scrutiny by the court.

POLITICAL USES OF ECHELON AND UKUSA



US National Security Agencies Remote Mind Control Head-Quarters at Menwith Hill, North Yorkshire, England.

Several incidents of domestic spying involving **ECHELON** have emerged from the secrecy of the UKUSA relationship. What these brief glimpses inside the intelligence world reveal is that, despite the best of intentions by elected representatives, presidents and prime ministers, the temptation to use **ECHELON** as a tool of political advancement and repression proves too strong.

Former Canadian spy Mike Frost recounts how former British Prime Minister Margaret Thatcher made a request in February 1983 to have two ministers from her own government monitored when she suspected them of disloyalty. In an effort to avoid the

legal difficulties involved with domestic spying on high-level governmental officials, the GCHQ liaison in Ottawa made a request to CSE for them to conduct the three-week-long surveillance mission at British taxpayer expense. Frost's CSE boss, Frank Bowman, travelled to London to do the job himself. After the mission was over, Bowman was instructed to hand over the tapes to a GCHQ official at head office.

Using the UKUSA alliance as legal cover is seductively easy. As Spyworld co-author Michel Gratton puts it:

"The Thatcher episode certainly shows that GCHQ, like NSA, found ways to put itself above the law and did not hesitate to get directly involved in helping a specific politician for her personal political benefit…

"[T]he decision to proceed with the London caper was probably not put forward for approval to many people up the bureaucratic ladder. It was something CSE figured they would get away with easily, so checking with the higher-ups would only complicate things unnecessarily."

Frost also told of how he was asked in 1975 to spy on an unlikely target: Prime Minister Pierre Trudeau's wife, Margaret Trudeau. The Royal Canadian Mounted Police's (RCMP) Security service division was concerned that the Prime Minister's wife was buying and using marijuana, so they contacted the CSE to do the dirty work. Months of surveillance in cooperation with the Security Service turned up nothing of note. Frost was concerned that there were political motivations behind the RCMP's request: "She was in no way suspected of espionage. Why was the RCMP so adamant about this? Were they trying to get at Pierre Trudeau for some reason or just protect him? Or were they working under orders from their political masters?"

The NSA frequently gets into the political spying act as well. Nixon presidential aide John Ehrlichman revealed in his published memoirs, Witness to Power: The Nixon Years, that Henry Kissinger used the NSA to intercept the messages of then Secretary of State William P. Rogers, which Kissinger used to convince President Nixon of Rogers' incompetence. Kissinger also found himself on the receiving end of the NSA's global net. Word of Kissinger's secret diplomatic dealings with foreign governments would reach the ears of other Nixon administration officials, incensing Kissinger. As former NSA Deputy Director William Colby pointed out: "Kissinger would get sore as hell…because he wanted to keep it politically secret until it was ready to launch."

However, elected representatives have also become targets of spying by the intelligence agencies. In 1988, Margaret Newsham, a former Lockheed software manager who was responsible for a dozen VAX computers that powered the **ECHELON** computers at Menwith Hill, came forth with the stunning revelation that she had actually heard the NSA's real-time interception of phone conversations involving South Carolina Senator Strom Thurmond. Newsham was fired from Lockheed after she filed a whistle-blower lawsuit alleging that the company was engaged in flagrant waste and abuse. After a top-secret meeting in April 1988 with then Chairman of the House Permanent Select Committee on Intelligence, Rep. Louis Stokes, Capitol Hill staffers familiar with the meeting leaked the story to the Cleveland Plain Dealer. While Sen. Thurmond was reluctant to pressure for a thorough investigation into the matter, his office revealed at the time that it had previously received reports that the Senator was a target of the NSA. After the news reports, an investigation into the matter discovered that there were no controls or questioning over who could enter target names into the Menwith Hill system.

The NSA, under orders from the Reagan Administration, also targeted Maryland Congressman Michael Barnes. Phone calls he placed to Nicaraguan officials were intercepted and recorded, including a conversation he had with the Foreign Minister of Nicaragua, protesting the implementation of martial law in that country. Barnes found out about the NSA's spying after White House officials leaked transcripts of his conversations to reporters. CIA Director William Casey, later implicated in the Iran-Contra affair, showed Barnes a Nicaraguan Embassy cable that reported a meeting between embassy staff and one of Barnes' aides. The aide had been there on a professional call regarding an international affairs issue, and Casey asked for Barnes to fire the aide. Barnes replied that it was perfectly legal and legitimate for his staff to meet with foreign diplomats. Barnes commented: "I was aware that NSA monitored international calls, that it was a standard part of intelligence gathering. But to use it for domestic political purposes is absolutely outrageous and probably illegal."

Another former chairman of the Senate Intelligence Committee has also expressed his concerns about the NSA's domestic targeting. "It has always worried me. What if that is used on American citizens?" queried former Arizona Senator Dennis DeConcini. "It is chilling. Are they listening to my private conversations on my telephone?"

Seemingly non-controversial organisations have ended up in the fixed gaze of **ECHELON**, as several former GCHQ officials confidentially told the London Observer in June 1992. Among the targeted organisations they named were Amnesty International, Greenpeace, and Christian Aid - an American missionary organisation that works with indigenous pastors engaged in ministry work in countries closed to Western, Christian workers.

In another story published by the London Observer, a former employee of the British Joint Intelligence Committee, Robin

Robison, admitted that Margaret Thatcher had personally ordered the communications interception of Lonrho, the parent company of the Observer, after the Observer had published a 1989 exposé charging that bribes had been paid to Thatcher's son, Mark, in a multibillion-dollar British arms deal with Saudi Arabia. Despite facing severe penalties for violating his indoctrination vows, Robison admitted that he had personally delivered intercepted Lonrho messages to Mrs Thatcher's office.

It should hardly be surprising that **ECHELON** ends up being used by elected and bureaucratic officials to their political advantage or by the intelligence agencies themselves for the purpose of sustaining their privileged surveillance powers and bloated budgets. The availability of such invasive technology practically begs for abuse, although it does not justify its use to those ends. But what is most frightening is the targeting of such "subversives" as those who expose corrupt government activity, protect human rights from government encroachments, challenge corporate polluters or promote the Gospel of Christ. That the vast intelligence powers of the United States should be arrayed against legitimate and peaceful organisations is demonstrative not of the desire to monitor, but of the desire to control.

COMMERCIAL SPYING

With the rapid erosion of the Soviet Empire in the early 1990s, Western intelligence agencies were anxious to redefine their mission to justify the scope of their global surveillance system. Some of the agencies' closest corporate friends quickly gave them an option: commercial espionage. By redefining the term "national security" to include spying on foreign competitors of prominent US corporations, the signals intelligence game has got uglier. And this may very well have prompted the recent scrutiny by the European Union that **ECHELON** has endured.

While UKUSA agencies have pursued economic and commercial information on behalf of their countries with renewed vigour after the passing of communism in Eastern Europe, the NSA practice of spying on behalf of US companies has a long history.

Gerald Burke, who served as Executive Director of President Nixon's Foreign Intelligence Advisory Board, notes commercial espionage was endorsed by the US Government as early as 1970: "By and large, we recommended that, henceforth, economic intelligence be considered a function of the national security, enjoying a priority equivalent to diplomatic, military and technological intelligence."

To accommodate the need for information regarding international commercial deals, the intelligence agencies set up a small, unpublicised department within the Department of Commerce: the Office of Intelligence Liaison. This office receives intelligence reports from the US intelligence agencies about pending international deals that it discreetly forwards to companies that request it or may have an interest in the information.

Immediately after coming to office in January 1993, President Clinton added to the corporate espionage machine by creating the National Economic Council, which feeds intelligence to "select" companies to enhance US competitiveness. The capabilities of **ECHELON** to spy on foreign companies is nothing new, but the Clinton Administration has raised its use to an art.

In 1990, the German magazine Der Spiegel revealed that the NSA had intercepted messages about an impending $200 million deal between Indonesia and the Japanese satellite manufacturer NEC Corp. After President Bush intervened in the negotiations on behalf of American manufacturers, the contract was split between NEC and AT&T.

In 1994, the CIA and NSA intercepted phone calls between Brazilian officials and the French firm Thomson-CSF about a radar system that the Brazilians wanted to purchase. The US firm Raytheon was a competitor as well, and was forwarded reports prepared from intercepts.

In September 1993, President Clinton asked the CIA to spy on Japanese auto manufacturers that were designing zero-emission cars and to forward that information to the Big Three US car manufacturers: Ford, General Motors and Chrysler. In 1995, the New York Times reported that the NSA and the CIA's Tokyo station were involved in providing detailed information to US Trade Representative Mickey Kantor's team of negotiators in Geneva, facing Japanese car companies in a trade dispute. Recently, the Japanese newspaper Mainichi accused the NSA of continuing to monitor the communications of Japanese companies on behalf of American companies.

Insight magazine reported in a series of articles in 1997 that President Clinton ordered the NSA and FBI to mount a massive surveillance operation at the 1993 Asia-Pacific Economic Cooperation (APEC) conference, held in Seattle. One intelligence source for the story related that over 300 hotel rooms had been bugged for the event - a move which was designed to obtain information regarding oil and hydro-electric deals pending in Vietnam, that was passed on to high-level Democratic Party contributors competing for the contracts.

But foreign companies were not the only losers. When Vietnam expressed interest in purchasing two used 737 freighter aircraft from an American businessman, the deal was scuttled after Commerce Secretary Ron Brown arranged favourable financing for two new 737s from Boeing.

But the US is not the only partner of the UKUSA relationship which engages in such activity. British Prime Minister Margaret Thatcher ordered the GCHQ to monitor the activities of international media mogul Robert Maxwell on behalf of the Bank of England.

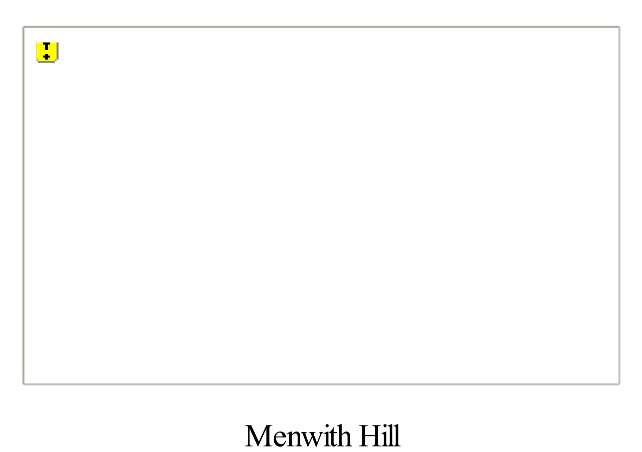
Former CSE linguist and analyst Jane Shorten claimed that she had seen intercepts from Mexican trade representatives during the 1992-1993 NAFTA trade negotiations, as well as 1991 South Korean Foreign Ministry intercepts dealing with the construction of three Canadian CANDU nuclear reactors for the Koreans in a US$6 billion deal. Shorten's revelation prompted Canadian Deputy Prime Minister Sheila Copps to launch a probe into the allegations after the Mexicans lodged a protest.

But every spy agency eventually gets beat at its own game. Mike Frost related in Spyworld how an accidental cellphone intercept in 1981, of the American Ambassador to Canada discussing a pending grain deal that the US was about to sign with China, provided Canada with the American negotiating strategy for the deal. The information was used to outbid the US, resulting in a three-year, $2.5 billion contract for the Canadian Wheat Board. CSE out-spooked the NSA again a year later when Canada snagged a $50-million wheat sale to Mexico.

Another disturbing trend regarding the present commercial use of **ECHELON** is the incestuous relationship that exists between the intelligence agencies and the US corporations that develop the technology that fuels their spy systems. Many of the companies that receive the most important commercial intercepts - Lockheed, Boeing, Loral, TRW and Raytheon - are actively involved in the manufacturing and operation of many of the spy systems that comprise **ECHELON**.

The collusion between intelligence agencies and their contractors is frightening in the chilling effect it has on creating any foreign or even domestic competition. But just as important is that it is a gross misuse of taxpayer-financed resources.

THE WARNING



Menwith Hill

The Menwith Hill facility is located in North Yorkshire, England, near Harrogate. The important role that Menwith Hill plays in the **ECHELON** system was recognised by the recent European Parliament STOA report:

Within Europe, all e-mail, telephone and fax communications are routinely intercepted by the United States National Security Agency, transferring all target information from the European mainland via the strategic hub of London, then by satellite to Fort Meade in Maryland via the crucial hub at Menwith Hill in the North Yorks Moors of the UK.

While the UKUSA relationship is a product of Cold War political and military tensions, **ECHELON** is purely a product of the 20th century - the century of "statism". The modern drive toward the assumption of state power has turned legitimate national security agencies and apparati into pawns in a manipulative game, where the stakes are no less than the survival of the Constitution. The systems developed prior to **ECHELON** were designed to confront the expansionist goals of the Soviet Empire - something the West was forced out of necessity to do.

But as Glyn Ford, European Parliament representative for Manchester, England, and the driving force behind the European investigation of **ECHELON**, has pointed out: "The difficulty is that the technology has now become so elaborate that what was originally a small client list has become the whole world."

What began as a noble alliance to contain and defeat the forces of communism has turned into a carte blanche to disregard the rights and liberties of the American people and the population of the free world. As has been demonstrated time and again, the NSA has been persistent in subverting not just the intent of the law in regard to the prohibition of domestic spying, but the letter as well. The laws that were created to constrain the intelligence agencies from infringing on our liberties are frequently flaunted, re-interpreted and revised according to the bidding and wishes of political spymasters in Washington, DC. Old habits die hard, it

seems.

As stated above, there is a need for such sophisticated surveillance technology. Unfortunately, the world is filled with criminals, drug lords, terrorists and dictators who threaten the peace and security of many nations. The thought that **ECHELON** can be used to eliminate or control these international thugs is heartening. But defenders of **ECHELON** argue that the rare intelligence victories over these forces of darkness and death give wholesale justification to indiscriminate surveillance of the entire world and every member of it. But more complicated issues than that remain.

The shameless and illegal targeting of political opponents, business competitors, dissidents and even Christian ministries stands as a testament that if we are to remain free, we must bind these intelligence systems and those that operate them with the heavy chains of transparency and accountability to our elected officials. But the fact that the **ECHELON** apparatus can be quickly turned around on those same officials in order to maintain some advantage for the intelligence agencies indicates that these agencies are not presently under the control of our elected representatives.

That Congress is not aware of or able to curtail these abuses of power is a frightening harbinger of what may come here in the United States. The European Parliament has begun the debate over what **ECHELON** is, how it is being used and how free countries should use such a system. The US Congress should join that same debate with the understanding that the consequences of ignoring or failing to address these issues could foster the demise of our republican form of government. Such is the threat, as Senator Frank Church warned the American people over twenty years ago: At the same time, that capability at any time could be turned around on the American people and no American would have any privacy left, such [is] the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide. If this government ever became a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back, because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know. Such is the capability of this technology…

I don't want to see this country ever go across the bridge. I know the capacity that is there to make tyranny total in America, and we must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that abyss. That is the abyss from which there is no return.

RECENT DEVELOPMENTS

Since this author's **ECHELON** report was first sent to the US Congress in November 1998, increased attention has been directed at the spy system by international media outlets and governmental representatives. As news of the system's sweeping technological capability comes to light, questions continue to be raised concerning the possible illicit uses of the system to circumvent domestic civil liberties protections.

The May 1999 publication of British investigator Duncan Campbell's detailed report, "Interception Capabilities 2000", for the European Parliament's Science and Technology Options Assessment Panel (STOA) continued to expose the scope of **ECHELON**'s supporting facilities and the reach of its surveillance technology. Among the report's key findings:

· While "word spotting" search systems have been previously thought to be widespread throughout the system, evidence indicates that this nascent technology is currently ineffective. However, **ECHELON** utilises speaker recognition system "voice-prints" to recognise the speech patterns of targeted individuals making international telephone calls.

· US law enforcement agencies are working with their European counterparts under the auspices of a previously secret organisation, ILETS (International Law Enforcement Telecommunications Seminar), to incorporate backdoor wiretapping capabilities into all existing forms of communications systems. In addition, the US Government is continuing to pursue diplomatic initiatives to convince other governments to adopt "key escrow" legislation requiring computer users to provide law enforcement agencies with encryption keys.

· The NSA continues to work with US software manufacturers to weaken the cryptographic capability of popular software programs, such as Lotus Notes and Internet browsers, to assist the intelligence agency in gaining access to a user's personal information.

· Intelligence sources reveal the increasing use of signals intelligence facilities to provide commercial advantages to domestic companies involved in international trade deals.

· The report provides original, new documentation about the **ECHELON** system and its role in the interception of

communications satellites. This includes details concerning how intelligence agencies are able to intercept Internet traffic and digital communications, including screen shots of traffic analysis from NSA computer systems.

Official UKUSA Confirmation

Privacy researchers were surprised in May when an Australian intelligence official confirmed the existence of the UKUSA intelligence-sharing treaty, in response to a formal information request by Channel 9 Sunday reporter Ross Coulthart. Martin Brady, director of the Defence Signals Directorate (DSD), admitted in a letter dated 16 March that his agency "does cooperate with counterpart signals intelligence organisations overseas under the UKUSA relationship".

Parliamentary and Congressional Inquiries

The growing concern about the use of **ECHELON** has finally extended to capitals and elected representatives around the world. Pressure from the international business community has been brought to bear on government officials in response to mounting evidence that industrial espionage by the US is costing European firms billions of dollars each year.

Germany also followed the French example in June, when the cabinet issued a policy statement encouraging its companies and citizens to utilise encryption programs without restrictions. German business leaders were alerted to the extent of US commercial spying after an anonymous NSA employee admitted on German television in August 1998 that he had participated in stealing industrial secrets from the wind generator manufacturer, Enercon, which were passed on to its main US competitor, Kenetech.

Perhaps the most important governmental development is the growing interest of members of the US Congress regarding **ECHELON** and its surveillance capabilities. Since the NSA is the prime mover in the UKUSA intelligence partnership, any hope of reining-in the activities of the US intelligence agencies will require the involvement of congressional oversight committees.

About the Author:

Patrick S. Poole is a lecturer in government and economics at Bannockburn College in Franklin, Tennessee, USA, having previously served as deputy Director of the Center for Technology Policy in Washington, DC. He contributes frequently to several publications on topics of privacy and civil liberties.

E-mail: **pspoole@hiwaay.net**

Website: **http://fly.hiway.net/~pspoole/echelon.html**

I fully believe that one day the (Anti-Society) ECHELON Citizen Spying Network will be dismantled by the people brick by brick just the same as the Berlin Wall.

George Farquhar (Oct 1999.)



ECHELON:

EXPOSING THE GLOBAL SURVEILLANCE SYSTEM

By Nicky Hager.

This article is reprinted with the permission of CAQ [to Ham Radio Online] (Covert Action Quarterly).

IN THE LATE 1980'S, IN A DECISION IT PROBABLY REGRETS, THE U.S. PROMPTED NEW ZEALAND TO JOIN A NEW AND HIGHLY SECRET GLOBAL INTELLIGENCE SYSTEM. HAGER'S INVESTIGATION INTO IT AND HIS DISCOVERY OF THE ECHELON DICTIONARY HAS REVEALED ONE OF THE WORLD'S BIGGEST, MOST CLOSELY HELD INTELLIGENCE PROJECTS. THE SYSTEM ALLOWS SPY AGENCIES TO MONITOR MOST OF THE WORLD'S TELEPHONE, E-MAIL, AND TELEX COMMUNICATIONS.

For 40 years, New Zealand's largest intelligence agency, the Government Communications Security Bureau (GCSB) the nation's equivalent of the US National Security Agency (NSA) had been helping its Western allies to spy on countries throughout the Pacific region, without the knowledge of the New Zealand public or many of its highest elected officials. What the NSA did not know is that by the late 1980s, various intelligence staff had decided these activities had been too secret for too long, and were providing me with interviews and documents exposing New Zealand's intelligence activities. Eventually, more than 50 people who work or have worked in intelligence and related fields agreed to be interviewed.

The activities they described made it possible to document, from the South Pacific, some alliance-wide systems and projects which have been kept secret elsewhere. Of these, by far the most important is **ECHELON**.

Designed and coordinated by NSA, the **ECHELON** system is used to intercept ordinary e-mail, fax, telex, and telephone communications carried over the world's telecommunications networks. Unlike many of the electronic spy systems developed during the Cold War, **ECHELON** is designed primarily for non-military targets: governments, organizations, businesses, and individuals in virtually every country. It potentially affects every person communicating between (and sometimes within) countries anywhere in the world.

It is, of course, not a new idea that intelligence organizations tap into e-mail and other public telecommunications networks. What was new in the material leaked by the New Zealand intelligence staff was precise information on where the spying is done, how the system works, its capabilities and shortcomings, and many details such as the codenames.

The **ECHELON** system is not designed to eavesdrop on a particular individual's e-mail or fax link. Rather, the system works by indiscriminately intercepting very large quantities of communications and using computers to identify and extract messages of interest from the mass of unwanted ones. A chain of secret interception facilities has been established around the world to tap into all the major components of the international telecommunications networks. Some monitor communications satellites, others land-based communications networks, and others radio communications. **ECHELON** links together all these facilities, providing

the US and its allies with the ability to intercept a large proportion of the communications on the planet.

The computers at each station in the **ECHELON** network automatically search through the millions of messages intercepted for ones containing pre-programmed keywords. Keywords include all the names, localities, subjects, and so on that might be mentioned. Every word of every message intercepted at each station gets automatically searched whether or not a specific telephone number or e-mail address is on the list.

The thousands of simultaneous messages are read in "real time" as they pour into the station, hour after hour, day after day, as the computer finds intelligence needles in telecommunications haystacks.

SOMEONE IS LISTENING:

The computers in stations around the globe are known, within the network, as the **ECHELON** Dictionaries. Computers that can automatically search through traffic for keywords have existed since at least the 1970s, but the **ECHELON** system was designed by NSA to interconnect all these computers and allow the stations to function as components of an integrated whole. The NSA and GCSB are bound together under the five-nation UKUSA signals intelligence agreement. The other three partners all with equally obscure names are the Government Communications Headquarters (GCHQ) in Britain, the Communications Security Establishment (CSE) in Canada, and the Defense Signals Directorate (DSD) in Australia.

The alliance, which grew from cooperative efforts during World War II to intercept radio transmissions, was formalized into the UKUSA agreement in 1948 and aimed primarily against the USSR. The five UKUSA agencies are today the largest intelligence organizations in their respective countries. With much of the world's business occurring by fax, e-mail, and phone, spying on these communications receives the bulk of intelligence resources. For decades before the introduction of the **ECHELON** system, the UKUSA allies did intelligence collection operations for each other, but each agency usually processed and analyzed the intercept from its own stations.

Under **ECHELON**, a particular station's Dictionary computer contains not only its parent agency's chosen keywords, but also has lists entered in for other agencies. In New Zealand's satellite interception station at Waihopai (in the South Island), for example, the computer has separate search lists for the NSA, GCHQ, DSD, and CSE in addition to its own. Whenever the Dictionary encounters a message containing one of the agencies' keywords, it automatically picks it and sends it directly to the headquarters of the agency concerned. No one in New Zealand screens, or even sees, the intelligence collected by the New Zealand station for the foreign agencies. Thus, the stations of the junior UKUSA allies function for the NSA no differently than if they were overtly NSA-run bases located on their soil.

The first component of the **ECHELON** network are stations specifically targeted on the international telecommunications satellites (Intelsats) used by the telephone companies of most countries. A ring of Intelsats is positioned around the world, stationary above the equator, each serving as a relay station for tens of thousands of simultaneous phone calls, fax, and e-mail. Five UKUSA stations have been established to intercept the communications carried by the Intelsats.

The British GCHQ station is located at the top of high cliffs above the sea at Morwenstow in Cornwall. Satellite dishes beside sprawling operations buildings point toward Intelsats above the Atlantic, Europe, and, inclined almost to the horizon, the Indian Ocean. An NSA station at Sugar Grove, located 250 kilometers southwest of Washington, DC, in the mountains of West Virginia, covers Atlantic Intelsats transmitting down toward North and South America. Another NSA station is in Washington State, 200 kilometers southwest of Seattle, inside the Army's Yakima Firing Center. Its satellite dishes point out toward the Pacific Intelsats and to the east.

The job of intercepting Pacific Intelsat communications that cannot be intercepted at Yakima went to New Zealand and Australia. Their South Pacific location helps to ensure global interception. New Zealand provides the station at Waihopai and Australia supplies the Geraldton station in West Australia (which targets both Pacific and Indian Ocean Intelsats).

Each of the five stations' Dictionary computers has a codename to distinguish it from others in the network. The Yakima station, for instance, located in desert country between the Saddle Mountains and Rattlesnake Hills, has the COWBOY Dictionary, while the Waihopai station has the FLINTLOCK Dictionary. These codenames are recorded at the beginning of every intercepted message, before it is transmitted around the **ECHELON** network, allowing analysts to recognize at which station the interception occurred.

New Zealand intelligence staff has been closely involved with the NSA's Yakima station since 1981, when NSA pushed the GCSB to contribute to a project targeting Japanese embassy communications. Since then, all five UKUSA agencies have been responsible for monitoring diplomatic cables from all Japanese posts within the same segments of the globe they are assigned for

general UKUSA monitoring. Until New Zealand's integration into **ECHELON** with the opening of the Waihopai station in 1989, its share of the Japanese communications was intercepted at Yakima and sent unprocessed to the GCSB headquarters in Wellington for decryption, translation, and writing into UKUSA-format intelligence reports (the NSA provides the codebreaking programs).

"COMMUNICATION" THROUGH SATELLITES:

The next component of the **ECHELON** system intercepts a range of satellite communications not carried by Intelsat.In addition to the UKUSA stations targeting Intelsat satellites, there are another five or more stations homing in on Russian and other regional communications satellites. These stations are Menwith Hill in northern England; Shoal Bay, outside Darwin in northern Australia (which targets Indonesian satellites); Leitrim, just south of Ottawa in Canada (which appears to intercept Latin American satellites); Bad Aibling in Germany; and Misawa in northern Japan.

A group of facilities that tap directly into land-based telecommunications systems is the final element of the **ECHELON** system. Besides satellite and radio, the other main method of transmitting large quantities of public, business, and government communications is a combination of water cables under the oceans and microwave networks over land. Heavy cables, laid across seabeds between countries, account for much of the world's international communications. After they come out of the water and join land-based microwave networks they are very vulnerable to interception. The microwave networks are made up of chains of microwave towers relaying messages from hilltop to hilltop (always in line of sight) across the countryside. These networks shunt large quantities of communications across a country. Interception of them gives access to international undersea communications (once they surface) and to international communication trunk lines across continents. They are also an obvious target for large-scale interception of domestic communications.

Because the facilities required to intercept radio and satellite communications use large aerials and dishes that are difficult to hide for too long, that network is reasonably well documented. But all that is required to intercept land-based communication networks is a building situated along the microwave route or a hidden cable running underground from the legitimate network into some anonymous building, possibly far removed. Although it sounds technically very difficult, microwave interception from space by United States spy satellites also occurs.4 The worldwide network of facilities to intercept these communications is largely undocumented, and because New Zealand's GCSB does not participate in this type of interception, my inside sources could not help either.

NO ONE IS SAFE FROM A MICROWAVE:

A 1994 expos of the Canadian UKUSA agency, Spyworld, co-authored by one of its former staff, Mike Frost, gave the first insights into how a lot of foreign microwave interception is done (see p. 18). It described UKUSA "embassy collection" operations, where sophisticated receivers and processors are secretly transported to their countries' overseas embassies in diplomatic bags and used to monitor various communications in foreign capitals.

Since most countries' microwave networks converge on the capital city, embassy buildings can be an ideal site. Protected by diplomatic privilege, they allow interception in the heart of the target country. *6 The Canadian embassy collection was requested by the NSA to fill gaps in the American and British embassy collection operations, which were still occurring in many capitals around the world when Frost left the CSE in 1990. Separate sources in Australia have revealed that the DSD also engages in embassy collection. On the territory of UKUSA nations, the interception of land-based telecommunications appears to be done at special secret intelligence facilities. The US, UK, and Canada are geographically well placed to intercept the large amounts of the world's communications that cross their territories.

The only public reference to the Dictionary system anywhere in the world was in relation to one of these facilities, run by the GCHQ in central London. In 1991, a former British GCHQ official spoke anonymously to Granada Television's World in Action about the agency's abuses of power. He told the program about an anonymous red brick building at 8 Palmer Street where GCHQ secretly intercepts every telex which passes into, out of, or through London, feeding them into powerful computers with a program known as "Dictionary." The operation, he explained, is staffed by carefully vetted British Telecom people: "It's nothing to do with national security. It's because it's not legal to take every single telex. And they take everything: the embassies, all the business deals, even the birthday greetings, they take everything. They feed it into the Dictionary." What the documentary did not reveal is that Dictionary is not just a British system; it is UKUSA-wide.

Similarly, British researcher Duncan Campbell has described how the US Menwith Hill station in Britain taps directly into the British Telecom microwave network, which has actually been designed with several major microwave links converging on an isolated tower connected underground into the station.

The NSA Menwith Hill station, with 22 satellite terminals and more than 4.9 acres of buildings, is undoubtedly the largest and most powerful in the UKUSA network. Located in northern England, several thousand kilometers from the Persian Gulf, it was awarded the NSA's "Station of the Year" prize for 1991 after its role in the Gulf War. Menwith Hill assists in the interception of microwave communications in another way as well, by serving as a ground station for US electronic spy satellites. These intercept microwave trunk lines and short range communications such as military radios and walkie talkies. Other ground stations where the satellites' information is fed into the global network are Pine Gap, run by the CIA near Alice Springs in central Australia and the Bad Aibling station in Germany. Among them, the various stations and operations making up the **ECHELON** network tap into all the main components of the world's telecommunications networks. All of them, including a separate network of stations that intercepts long distance radio communications, have their own Dictionary computers connected into **ECHELON**.

In the early 1990s, opponents of the Menwith Hill station obtained large quantities of internal documents from the facility. Among the papers was a reference to an NSA computer system called Platform. The integration of all the UKUSA station computers into **ECHELON** probably occurred with the introduction of this system in the early 1980s. James Bamford wrote at that time about a new worldwide NSA computer network codenamed Platform "which will tie together 52 separate computer systems used throughout the world. Focal point, or `host environment,' for the massive network will be the NSA headquarters at Fort Meade. Among those included in Platform will be the British SIGINT organization, GCHQ."

LOOKING IN THE DICTIONARY:

The Dictionary computers are connected via highly encrypted UKUSA communications that link back to computer data bases in the five agency headquarters. This is where all the intercepted messages selected by the Dictionaries end up. Each morning the specially "indoctrinated" signals intelligence analysts in Washington, Ottawa, Cheltenham, Canberra, and Wellington log on at their computer terminals and enter the Dictionary system. After keying in their security passwords, they reach a directory that lists the different categories of intercept available in the data bases, each with a four-digit code. For instance, 1911 might be Japanese diplomatic cables from Latin America (handled by the Canadian CSE), 3848 might be political communications from and about Nigeria, and 8182 might be any messages about distribution of encryption technology.

They select their subject category, get a "search result" showing how many messages have been caught in the **ECHELON** net on that subject, and then the day's work begins. Analysts scroll through screen after screen of intercepted faxes, e-mail messages, etc. and, whenever a message appears worth reporting on, they select it from the rest to work on. If it is not in English, it is translated and then written into the standard format of intelligence reports produced anywhere within the UKUSA network either in entirety as a "report," or as a summary or "gist."

INFORMATION CONTROL:

A highly organized system has been developed to control what is being searched for by each station and who can have access to it. This is at the heart of **ECHELON** operations and works as follows.

The individual station's Dictionary computers do not simply have a long list of keywords to search for. And they do not send all the information into some huge database that participating agencies can dip into as they wish. It is much more controlled.

The search lists are organized into the same categories, referred to by the four digit numbers. Each agency decides its own categories according to its responsibilities for producing intelligence for the network. For GCSB, this means South Pacific governments, Japanese diplomatic, Russian Antarctic activities, and so on.

The agency then works out about 10 to 50 keywords for selection in each category. The keywords include such things as names of people, ships, organizations, country names, and subject names. They also include the known telex and fax numbers and Internet addresses of any individuals, businesses, organizations, and government offices that are targets. These are generally written as part of the message text and so are easily recognized by the Dictionary computers.

The agencies also specify combinations of keywords to help sift out communications of interest. For example, they might search for diplomatic cables containing both the words "Santiago" and "aid," or cables containing the word "Santiago" but not "consul" (to avoid the masses of routine consular communications). It is these sets of words and numbers (and combinations), under a particular category, that get placed in the Dictionary computers. (Staff in the five agencies called Dictionary Managers enter and update the keyword search lists for each agency.)

The whole system, devised by the NSA, has been adopted completely by the other agencies. The Dictionary computers search through all the incoming messages and, whenever they encounter one with any of the agencies' keywords, they select it. At the

same time, the computer automatically notes technical details such as the time and place of interception on the piece of intercept so that analysts reading it, in whichever agency it is going to, know where it came from, and what it is. Finally, the computer writes the four-digit code (for the category with the keywords in that message) at the bottom of the message's text. This is important. It means that when all the intercepted messages end up together in the database at one of the agency headquarters, the messages on a particular subject can be located again. Later, when the analyst using the Dictionary system selects the four-digit code for the category he or she wants, the computer simply searches through all the messages in the database for the ones which have been tagged with that number.

This system is very effective for controlling which agencies can get what from the global network because each agency only gets the intelligence out of the **ECHELON** system from its own numbers. It does not have any access to the raw intelligence coming out of the system to the other agencies. For example, although most of the GCSB's intelligence production is primarily to serve the UKUSA alliance, New Zealand does not have access to the whole **ECHELON** network. The access it does have is strictly controlled. A New Zealand intelligence officer explained: "The agencies can all apply for numbers on each other's Dictionaries. The hardest to deal with are the Americans. ... [There are] more hoops to jump through, unless it is in their interest, in which case they'll do it for you."

There is only one agency which, by virtue of its size and role within the alliance, will have access to the full potential of the **ECHELON** system the agency that set it up. What is the system used for? Anyone listening to official "discussion" of intelligence could be forgiven for thinking that, since the end of the Cold War, the key targets of the massive UKUSA intelligence machine are terrorism, weapons proliferation, and economic intelligence. The idea that economic intelligence has become very important, in particular, has been carefully cultivated by intelligence agencies intent on preserving their post-Cold War budgets. It has become an article of faith in much discussion of intelligence. However, I have found no evidence that these are now the primary concerns of organizations such as NSA.

QUICKER INTELLIGENCE, SAME MISSION:

A different story emerges after examining very detailed information I have been given about the intelligence New Zealand collects for the UKUSA allies and detailed descriptions of what is in the yards-deep intelligence reports New Zealand receives from its four allies each week. There is quite a lot of intelligence collected about potential terrorists, and there is quite a lot of economic intelligence, notably intensive monitoring of all the countries participating in GATT negotiations. But by far, the main priorities of the intelligence alliance continue to be political and military intelligence to assist the larger allies to pursue their interests around the world. Anyone and anything the particular governments are concerned about can become a target.

With capabilities so secret and so powerful, almost anything goes. For example, in June 1992, a group of current "highly placed intelligence operatives" from the British GCHQ spoke to the London Observer: "We feel we can no longer remain silent regarding that which we regard to be gross malpractice and negligence within the establishment in which we operate." They gave as examples GCHQ interception of three charitable organizations, including Amnesty International and Christian Aid. As the Observer reported: "At any time GCHQ is able to home in on their communications for a routine target request," the GCHQ source said. In the case of phone taps the procedure is known as Mantis. With telexes it is called Mayfly. By keying in a code relating to Third World aid, the source was able to demonstrate telex "fixes" on the three organizations. "It is then possible to key in a trigger word which enables us to home in on the telex communications whenever that word appears," he said. "And we can read a pre-determined number of characters either side of the keyword." Without actually naming it, this was a fairly precise description of how the **ECHELON** Dictionary system works. Again, what was not revealed in the publicity was that this is a UKUSA-wide system. The design of **ECHELON** means that the interception of these organizations could have occurred anywhere in the network, at any station where the GCHQ had requested that the four-digit code covering Third World aid be placed.

Note that these GCHQ officers mentioned that the system was being used for telephone calls. In New Zealand, **ECHELON** is used only to intercept written communications: fax, e-mail, and telex. The reason, according to intelligence staff, is that the agency does not have the staff to analyze large quantities of telephone conversations.

Mike Frost's expos of Canadian "embassy collection" operations described the NSA computers they used, called Oratory, that can "listen" to telephone calls and recognize when keywords are spoken. Just as we can recognize words spoken in all the different tones and accents we encounter, so too, according to Frost, can these computers. Telephone calls containing keywords are automatically extracted from the masses of other calls and recorded digitally on magnetic tapes for analysts back at agency headquarters. However, high volume voice recognition computers will be technically difficult to perfect, and my New Zealand-based sources could not confirm that this capability exists. But, if or when it is perfected, the implications would be immense. It

would mean that the UKUSA agencies could use machines to search through all the international telephone calls in the world, in the same way that they do written messages. If this equipment exists for use in embassy collection, it will presumably be used in all the stations throughout the **ECHELON** network. It is yet to be confirmed how extensively telephone communications are being targeted by the **ECHELON** stations for the other agencies.

The easiest pickings for the **ECHELON** system are the individuals, organizations, and governments that do not use encryption. In New Zealand's area, for example, it has proved especially useful against already vulnerable South Pacific nations which do not use any coding, even for government communications (all these communications of New Zealand's neighbors are supplied, unscreened, to its UKUSA allies). As a result of the revelations in my book, there is currently a project under way in the Pacific to promote and supply publicly available encryption software to vulnerable organizations such as democracy movements in countries with repressive governments. This is one practical way of curbing illegitimate uses of the **ECHELON** capabilities.

One final comment. All the newspapers, commentators, and "well placed sources" told the public that New Zealand was cut off from US intelligence in the mid-1980s. That was entirely untrue. The intelligence supply to New Zealand did not stop, and instead, the decade since has been a period of increased integration of New Zealand into the US system. Virtually everything the equipment, manuals, ways of operating, jargon, codes, and so on, used in the GCSB continues to be imported entirely from the larger allies (in practice, usually the NSA). As with the Australian and Canadian agencies, most of the priorities continue to come from the US, too.

The main thing that protects these agencies from change is their secrecy. On the day my book arrived in the book shops, without prior publicity, there was an all-day meeting of the intelligence bureaucrats in the prime minister's department trying to decide if they could prevent it from being distributed. They eventually concluded, sensibly, that the political costs were too high. It is understandable that they were so agitated.

Throughout my research, I have faced official denials or governments refusing to comment on publicity about intelligence activities. Given the pervasive atmosphere of secrecy and stonewalling, it is always hard for the public to judge what is fact, what is speculation, and what is paranoia. Thus, in uncovering New Zealand's role in the NSA-led alliance, my aim was to provide so much detail about the operations the technical systems, the daily work of individual staff members, and even the rooms in which they work inside intelligence facilities that readers could feel confident that they were getting close to the truth. I hope the information leaked by intelligence staff in New Zealand about UKUSA and its systems such as **ECHELON** will help lead to change.

MORE FACTS ON THE ANTI-SOCIETY ECHELON GLOBAL CITIZEN SURVEILLANCE SYSTEM

http://mediafilter.org/caq
http://www.worldmedia.com/caq

3 and 16 March 1998: Link to original sources on **ECHELON**

2 February 1998
Source: http://206.13.40.11/1996/dec/ECHELON.html

I fully believe that one day the (Anti-Society) ECHELON Citizen Spying Network will be dismantled by the people brick by brick just the same as the Berlin Wall.

George Farquhar (Oct 1999.)

PREVIOUS	HOME	CONTINUE



ECHELON:

THEY'VE GOT IT TAPED

By Duncan Campbell

. . . and they don't give a damn about personal privacy or commercial confidence.Project 415 is a top-secret new global surveillance system. It can tap into a billion calls a year in the UK alone. Inside Duncan Campbell on how spying entered the 21st century . . .

In the booming surveillance industry they spy on whom they wish, when they wish, protected by barriers of secrecy, fortified by billions of pounds worth of high, high technology. Duncan Campbell reports from the United States on the secret Anglo-American plan for a global electronic spy system for the 21st century capable of listening in to most of us most of the time.

American, British and Allied intelligence agencies are soon to embark on a massive, billion-dollar expansion of their global electronic surveillance system. According to information given recently in secret to the US Congress, the surveillance system will enable the agencies to monitor and analyse civilian communications into the 21st century. Identified for the moment as Project P415, the system will be run by the US National Security Agency (NSA). But the intelligence agencies of many other countries will be closely involved with the new network, including those from Britain, Australia, Germany and Japan--and, surprisingly, the People's Republic of China.

New satellite stations and monitoring centres are to be built around the world, and a chain of new satellites launched, so that NSA and its British counterpart, the Government Communications Headquarters (GCHQ) at Cheltenham, may keep abreast of the burgeoning international telecommunications traffic.

The largest overseas station in the Project P415 network is the US satellite and communications base at Menwith Hill. near Harrogate in Yorkshire. It is run undercover by the NSA and taps into all Britain's main national and international communications networks (*New Statesman*, 7 August 1980). Although high technology stations such as Menwith Hill are primarily intended to monitor international communications, according to US experts their capability can be, and has been, turned inwards on domestic traffic. Menwith Hill, in particular, has been accused by a former employee of gross corruption and the monitoring of domestic calls.

The vast international global eavesdropping network has existed since shortly after the second world war, when the US, Britain, Canada, Australia and New Zealand signed a secret agreement on signals intelligence, or "sigint". It was anticipated, correctly, that electronic monitoring of communications signals would continue to be the largest and most important form of post-war secret intelligence, as it had been through the war.

Although it is impossible for analysts to listen to all but a small fraction of the billions of telephone calls, and other signals which might contain "significant" information, a network of monitoring stations in Britain and elsewhere is able to tap all international and

some domestic communications circuits, and sift out messages which sound interesting. Computers automatically analyse every telex message or data signal, and can also identify calls to, say, a target telephone number in London, no matter from which country they originate.

A secret listening agreement, called UKUSA (UK-USA), assigns parts of the globe to each participating agency. GCHQ at Cheltenham is the co-ordinating centre for Europe, Africa and the Soviet Union (west of the Ural Mountains).

The NSA covers the rest of the Soviet Union and most of the Americas. Australia--where another station in the NSA listening network is located in the outback--co-ordinates the electronic monitoring of the South Pacific, and South East Asia.

With 15,000 staff and a budget of over £500 million a year (even without the planned new Zircon spy satellite), GCHQ is by far the largest part of British intelligence. Successive UK governments have placed high value on its eavesdropping capabilities, whether against Russian military signals or the easier commercial and private civilian targets.

Both the new and existing surveillance systems are highly computerised. They rely on near total interception of international commercial and satellite communications in order to locate the telephone or other messages of target individuals. Last month, a US newspaper, the *Cleveland Plain Dealer*, revealed that the system had been used to target the telephone calls of a US Senator, Strom Thurmond. The fact that Thurmond, a southern Republican and usually a staunch supporter of the Reagan administration, is said to have been a target has raised fears that the NSA has restored domestic, electronic, surveillance programmes. These were originally exposed and criticised during the Watergate investigations, and their closure ordered by President Carter.

After talking to the NSA, Thurmond later told the *Plain Dealer* that he did not believe the allegation. But Thurmond, a right-wing Republican, may have been unwilling to rock the boat. Staff members of the Permanent Select Committee on Intelligence said that staff were "digging into it" despite the "stratospheric security classification" of all the systems involved.

The Congressional officials were first told of the Thurmond interception by a former employee of the Lockheed Space and Missiles Corporation, Margaret Newsham, who now lives in Sunnyvale, California. Newsham had originally given separate testimony and filed a lawsuit concerning corruption and mis-spending on other US government "black" projects. She has worked in the US and Britain for two corporations which manufacture signal intelligence computers, satellites and interception equipment for NSA, Ford Aerospace and Lockheed. Citing a special Executive Order signed by President Reagan. she told me last month that she could not and would not discuss classified information with journalists. But according to Washington sources (and the report in the *Plain Dealer*, she informed a US Congressman that the Thurmond interception took place at Menwith Hill, and that she personally heard the call and was able to pass on details.

Since then, investigators have subpoenaed other witnesses and asked them to provide the complete plans and manuals of the ECHELON system and related projects. The plans and blueprints are said to show that targeting of US political figures would not occur by accident. but was designed into the system from the start.

While working at Menwith Hill, Newsham is reported to have said that she was able to listen through earphones to telephone calls being monitored at the base. Other conversations that she heard were in Russian. After leaving Menwith Hill, she continued to have access to full details of Menwith Hill operations from a position as software manager for more than a dozen VAX computers at Menwith which operate the ECHELON system.

Newsham refused last month to discuss classified details of her career, except with cleared Congressional officials. But it has been publicly acknowledged that she worked on a large range of so-called "black" US intelligence programmes, whose funds are concealed inside the costs of other defence projects. She was fired from Lockheed four years ago after complaining about the corruption, and sexual harassment.

Lockheed claimed she had been a pook *[as written]* timekeeper, and has denied her charges of corruption on "black" projects. But the many charges she is reported to have made--such as the use of top secret computers for football pools, or to sell a wide range of merchandise from their offices, and deliberate and massive overcharging and waste by the company--are but small beer in a continuing and wider scandal about defence procurement. Newsham's testimony about overcharging by contractors is now the subject of a major congressional inquiry.

From US sources not connected with Margaret Newsham, we have obtained for the first time a list of the major classified projects in operation at Menwith Hill. The base currently has over 1,200 staff, more than two thirds of them Americans. Other than the ECHELON computer network, the main projects at Menwith Hill are code-named SILKWORTH, MOONPENNY, SIRE, RUNWAY and STEEPLEBUSH. The station also receives information from a satellite called BIG BIRD.

Project SILKWORTH is, according to signals intelligence specialists, the code-name for long-range radio monitoring from Menwith Hill. MOONPENNY is a system for monitoring satellite communications; RUNWAY is thought to be the control network for an eavesdropping satellite called VORTEX, now in orbit over the Soviet Union The base earlier controlled a similar series of satellites called CHALET. The new STEEPLEBUSH control centre appears connected with the latest and biggest of the overhead listening satellites. These are code-named MAGNUM, according to US intelligence sources.

BIG BIRD, which is not usually connected with Menwith Hill, is a low-orbiting photographic reconnaissance satellite. But investigators have worked out, from details of the clearances necessary to know about BIG BIRD, that this satellite--and indeed, many other satellites, variously disguised as "weather satellites"--also carry listening equipment. One such sigint package is said to have been aboard the doomed space shuttle Challenger, despite its ostensibly civilian purpose.

Recently published US Department of Defense 1989 budget information has confirmed that the Menwith Hill spy base will be the subject of a major $26 million expansion programme. Information given to Congress in February listed details of plans for a four-year expansion of the main operation building and other facilities at Menwith Hill. Although the testimony referred only to a "classified location", the base can be identified because of references to STEEPLEBUSH. According to this testimony, the new STEEPLEBUSH II project will cost $15 million between now and 1993. The expansion is required to avoid overcrowding and "to support expanding classified missions".

During the Watergate affair. it was revealed that NSA, in collaboration with GCHQ, had routinely intercepted the international communications of prominent anti-Vietnam war leaders such as Jane Fonda and Dr Benjamin Spock. Another target was former Black Panther leader Eldridge Cleaver. Then in the late 1970s, it was revealed that President Carter had ordered NSA to stop obtaining "back door" intelligence about US political figures through swapping intelligence data with GCHQ Cheltenham.

Among important stations being developed in the new P415 network, sources indicated, are Bude in Cornwall, mainly run by GCHQ, Bad Aibling in Germany, and two sites in the People's Republic of China (which are used only for monitoring the USSR). The western intelligence agencies have not yet resolved the question of how to replace the recently upgraded British intelligence listening station at Chung Hom Kok in Hong Kong (which at the moment listens to China itself) when the colony is handed back to China next decade.

In Australia three months ago, New Zealand Defence Minister Bob Tizard revealed that two Australasian interception stations planned for the early 1990s will be targeted on new communications satellites launched by third world countries such as India and Indonesia. The new satellite spy bases are at Geraldton in northern Australia and Blenheim, New Zealand. The similar British spy base at Morwenstow, near Bude, Cornwall, has been continuously expanded throughout the 1980s, including the provision of massive US analysis computers.

If Margaret Newsham's testimony is confirmed by the ongoing Congressional investigation, then the NSA has been behaving illegally under US law--unless it can prove either that Thurmond's call was intercepted completely accidentally, or that the highly patriotic Senator is actually a foreign spy or terrorist. Moreover NSA's international phone tapping operations from Menwith Hill and at Morwenstow, Cornwall, can only be legal in Britain if special warrants have been issued by the Secretary of State to specify that American intelligence agents are persons to whom information from intercepts must or should be given. This can not be established, since the government has always refused to publish any details of the targets or recipients of specific interception warrants.

When the Menwith Hill base was first set up there was no British law controlling phone tapping, or making unauthorised interception (such as by foreign intelligence agencies) illegal. Now there is, and telecommunications interception by the Americans from British territory would clearly be illegal without the appropriate warrant.

When the new Interception of Communications Act was passed in 1985, however, it was obviously designed to make special provision for operations like ECHELON or Project P415 to trawl all international communications to and from Britain. A special section of the Act, Section 3(2), allows warrants to be issued to intercept any general type of international messages to or from Britain if this is "in the interests of national security" or "for the purpose of safeguarding the economic well-being of the United Kingdom". Such warrants also allow GCHQ to tap any or all other communications on the same cables or satellites that may have to be picked up in order to select out the messages they want. So whether or not a British government warrant can legally allow American agents to intercept private British communications, there is no doubt that British law as well as British bases have been designed to encourage rather than inhibit the booming industry in international telecommunications surveillance.

Both British and American domestic communications are also being targeted and intercepted by the ECHELON network, the US investigators have been told. The agencies are alleged to have collaborated not only on targeting and interception, but also on

the monitoring of domestic UK communications.

Special teams from GCHQ Cheltenham have been flown in secretly in the last few years to a computer centre in Silicon Valley near San Francisco for training on the special computer systems that carry out both domestic and international interception.

The centre near San Francisco has also been used to train staff from the "Technical Department" of the People's Liberation Army General Staff, which is the Chinese version of GCHQ. The Department operates two ultra-secret joint US-Chinese listening stations in the Xinjiang Uighur Autonomous Region, close to the Soviet Siberian border. Allegedly, such surveillance systems are only used to target Soviet or Warsaw Pact communications signals, and those suspected of involvement in espionage and terrorism. But those involved in ECHELON have stressed to Congress that there are no formal controls over who may be targeted. And I have been told that junior intelligence staff can feed target names into the system at all levels, without any check on their authority to do so. Witnesses giving evidence to the Congressional inquiry have discussed whether the Democratic presidential contender Jesse Jackson was targeted; one source implied that he had been. Even test engineers from manufacturing companies are able to listen in on private citizens' communications, the inquiry was told.

But because of the special Executive Order signed by President Reagan, US intelligence operatives who know about such politically sensitive operations face jail sentences if they speak out--despite the constitutional American protection of freedom of speech and of the press. And in Britain, as we know, the government is in the process of tightening the Official Secrets Act to make the publication of any information from intelligence officials automatically a crime, even if the information had already been published, or had appeared overseas first.

MORE FACTS ON THE ANTI-SOCIETY ECHELON GLOBAL CITIZEN SURVEILLANCE SYSTEM

Note: Duncan Campbell has generously provided additional US sources of information on electronic inteception which shall be offered on this site when available.

Selected references:

1972 Winslow Peck, former NSA analyst, *Ramparts* interview on NSA electronic interception: http://jya.com/nsa-elint.htm (89K)

1973 Anonymous, "Uncle Sam and His 40,000 Snoopers," Nation Review (AU): http://jya.com/nsa-40k.htm

1975 US Senate (Church Report), "The National Security Agency and 4th Amendment Rights," Part 1: http://jya.com/nsa-4th.htm

1975 US Senate (Church Report), "The National Security Agency and 4th Amendment Rights," Part 2: http://jya.com/nsa-4th-p2.htm

1976 Duncan Campbell, "British MP Accuses U.S. of Electronic spying," *New Scientist*, August 5, 1976, p. 268.

1979 Duncan Campbell, "The Threat of the Electronic Spies," *New Statesman*, February 2, 1979, pp. 140-44.

1980 Duncan Campbell, "Society Under Surveillance," *Policing The Police,* Vol. 2. (Ed: Ha.) John Calder, London.

1980 Duncan Campbell and Clive Thomas, "BBC's Trade Secrets," *New Statesman*, July 4, 1980, pp. 13-14.

1980 Duncan Campbell and Linda Melvern, "America's Big Ear on Europe," *New Statesman,* July 18, 1980, pp. 10-14.

1981 Duncan Campbell, (Ed.) "Big Brother Is Listening - Phone tappers and the security state", 1st ed. Vol. 2. *New Statesman*, London.

1983 Duncan Campbell, "Spy in the Sky," *New Statesman,* September 9, 1983, pp. 8-9.

1983 James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency,* London, Penguin. Excerpts:

Chapter 8 - Partners (76K)

Chapter 9 - Competition (69K)
Chapter 10 - Abyss (43K)

1984 Duncan Campbell, *The Unsinkable Aircraft Carrier: American Military Power in Britain*, London, Michael Joseph.

1985 Jeffrey T. Richelson and Desmond Ball, *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries,* London, Allen & Unwin.

1986 Duncan Campbell and Patrick Forbes, "UK's Listening Link to Apartheid," *New Statesman*, August 1, 1986, pp. 101-11.

1986 Duncan Campbell and S. Connor, *On The Record*, Michael Joseph, London.

1987 William Burrows, *Deep Black: Space Espionage and National Security*, New York, Random House. Excerpt:

Chapter 8 - Foreign Bases: A Net Spread Wide (71K)

1989 Jeffrey T. Richelson, *The U.S. Intelligence Community*, New York, Ballinger. Excerpts:

Chapter 8 - Signals Intelligence (97K)
Chaper 12 - Exchange and Liaison Arrangements (72K)

1994, *Spyworld*, co-author Mike Frost, formerly agent with Canada's Communication Security Establisment (CSE), Doublday. See following item for more on Frost's espionage revelations.

1996 Nicky Hager, *Secret Power*: *New Zealand's Role In the International Spy Network*, Craig Potton, Nelson, New Zealand.

Chapter 2, Hooked up to the spy network: The UKUSA system

1996 *Intelligence Online* report on UKUSA cooperation: http://www.blythe.org/Intelligence/readme/brits-usa.int45

1997 *Daily Telegraph* report "Spies Like US" on Mentwith Hill (with aerial photo) and other commentary: http://www.accessone.com/~rivero/POLITICS/ECHELON/echelon.html

1998 Nicky Hager, *Covert Action Quarterly* article on ECHELON: http://jya.com/echelon.htm (30K)

1998 European Parliament, STOA report, *Assessment of the Technologies of Political Control*: http://jya.com/stoa-atpc.htm (295K)

1999 http://www.europarl.eu.int/dg4/stoa/en/news/1999/may99.htm

Development of surveillance technology and risk of abuse of economic information (Appraisal of technologies of political control)

(1) The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception; Survey of opinions of experts, by Nikos BOGONIKOLOS, Zeus E.E.I.G, Patras, Greece Interim Study, Working document for the STOA Panel, Workplan 1998 - 98/14/01, EN, May 1999, PE 168.184/Int.St./Part 1/4

(2) The legality of the interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law, by Chris ELLIOTT, Surrey, UK Final Study, Working document for the STOA Panel, Workplan 1998 - 8/14/01, EN, April 1999, PE 168.184/part 2/4

(3) Encryption and cryptosystems in electronic surveillance: A survey of the technology assessment issues, by Franck LEPRÉVOST, Technische Universität Berlin, Germany Final Study, Working document for the STOA Panel, Workplan 1998 - 98/14/01, EN, April 1999, PE 168.184/part 3/4

(4) The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition, by Duncan CAMPBELL, IPTV Ltd., Edinburgh, UK Final

Study, Working document for the STOA Panel, Workplan 1998 - 98/14/01, EN, April 1999, PE 168.184/part 4/4:

http://www.iptvreports.mcmail.com/stoa_cover.htm

Or a mirror at JYA, Zipped by Duncan Campbell for your convenience:

http://jya.com/ic2000.zip (961K)

The National Security Agency Web site: http://www.nsa.gov:8080/

Related US Office of Technology Assessment reports on electronic surveillance, 1972-1996: http://jya.com/esnoop.htm

---

I fully believe that one day the (Anti-Society) ECHELON Citizen Spying Network will be dismantled by the people brick by brick just the same as the Berlin Wall.

George Farquhar (Oct 1999.)

PREVIOUS	HOME	